

Vital Information
For Your
Organization

The Toll Fraud Files

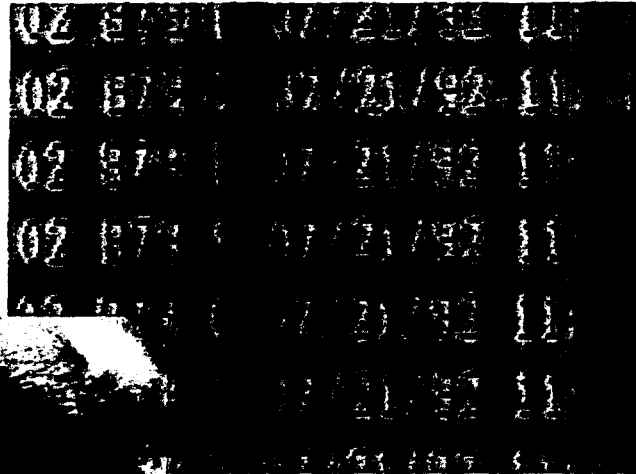
Case Study #1: The Voice Mail Marauders

Toll abusers victimized a Colorado organization by setting up a call-sell operation from pay telephones in New York City and suburban New Jersey.

How They Did It

The perpetrators called into the organization's voice mail system on its own 800 lines. Once inside, they hacked access codes until achieving a "hit." With the valid code, they were able to transfer calls through the voice mail system's automated attendant feature to the public switched network.

Because the system allowed unrestricted outbound long distance calling, "customers" of the call-sell operation were able to place hundreds



of unauthorized calls to Central America and the Dominican Republic. The hackers collected the cash, then vanished when their scheme was uncovered.

The Victim's Loss

Financial loss to the organization: \$20,000 over a six-day period.

Continued on reverse side

USWEST
COMMUNICATIONS 
Making the most of your time.®

How the Victim Responded

The tip-off to toll fraud was a high volume of incoming 800 calls from New York and New Jersey—areas not ordinarily served by the Colorado organization. Subsequent investigation—with the assistance of U S WEST Communications—revealed the magnitude of the problem.

To safeguard itself from further fraud, the organization:

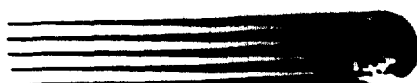
- eliminated outgoing long distance trunk access through its voice mail system
- re-programmed its voice mail system to invalidate calls that employed the outgoing trunk access code
- restricted its Automatic Route Selection (ARS) feature to disallow international long distance calling

**U S WEST Communications:
Dedicated To Fighting Toll Fraud**

USWEST
COMMUNICATIONS 
Making the most of your time.®

ATTACHMENT C

USWEST Express Calling



Dear US WEST Express Calling Card Customer:

We are pleased to provide you with the new US WEST Express Calling Card. It's the easy, convenient way to make calls while away from home. Here's why:

THE CARD THAT'S EASY TO USE

- The US WEST Express Calling Card number is, in most cases, your home telephone number and a four-digit security code you can choose yourself (any number from 2000 to 9999).
- There are no long, cumbersome numbers to memorize. You simply dial "0", enter the number you're calling, wait for a tone, then enter your US WEST Express Calling Card number.
- The card works in most card-reader phones. Just insert your card in the slot according to the directions on the phone and enter the number you're calling.

THE CARD THAT'S ACCEPTED ANYWHERE

No matter where you travel you can use your US WEST Express Calling Card with confidence. It's accepted almost anywhere, anytime, on almost every phone; across town or around the world.

THE CARD THAT SAVES YOU MONEY

Using the US WEST Express Calling Card to make your local and long distance calls when you're away from home costs less than bill-to-third or collect calls. There is no charge for the card and no annual fees.*

THE CARD THAT'S MORE SECURE

Even if it's lost or stolen, your US WEST Express Calling Card is secure because your security code is not printed on the card. Please read the enclosed information for more tips on keeping your card safe from fraud.

The ease and convenience of the Express Calling Card is one more way US WEST Communications is helping you make the most of your time. If you want to order additional cards, or choose your personalized security code, please call your local business office.

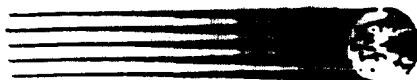
Sincerely,

Lori Vienneau
US WEST Communications

* A calling card surcharge applies in addition to local or long distance usage charges.

Please see other side for Card Holder Agreement

USWEST Express Calling



J. Q. PUBLIC
1 MAIN STREET
ANYWHERE, USA

The only card you need:

Easy

The card number, in most cases, is your phone number and a security code you can choose yourself.

Convenient

No long access codes to memorize.

Universal

The card is accepted by most long distance companies to place calls anywhere from almost any phone.

Secure

For your protection, your security code is not printed on your card. To further insure against fraud, follow the simple guidelines below.

How to use your Express Calling Card for local and long distance calls.

Touch tone phones

1. Enter "0"
2. Enter the number you wish to reach.
3. Listen for a tone.
4. Enter your card number, including your security code. (Rotary phones, wait for operator, then give card number and security code.)

Card reader phones

1. Insert and remove card according to instructions on the phone.
2. Wait for the next dial tone.
3. Dial "0" and the number you wish to reach.

Tip:

If the number you're calling is the same as your card number, you only need to enter your security code.

Your card number is ▼

M/11 1 402 555 1234

Protect your card against fraud:

1. Use a card reader phone whenever available.
2. Position yourself so that persons standing near you can not watch you dial or hear you speak your security code.
3. Never give your security code to anyone calling you, even if they identify themselves as phone company employees, law enforcement agency representatives, or long distance security personnel.
4. Examine your monthly bill.
5. Call the appropriate number on the back of your Security Card immediately if you suspect fraud on your card.

Security Card
If your card is lost or stolen, please
call the appropriate toll free number
on the back of this card.

This is your unique
Security Code

Security Card
If your card is lost or stolen, please
call the appropriate toll free number
on the back of this card.

This is your unique
Security Code

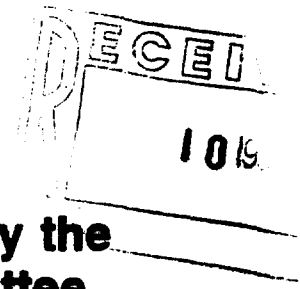
ATTACHMENT D

1- 7-94
no date

AK

CC 93-272 CKS
Circuit mule

**A Cooperative Solution to the Fraud that Targets
Telecom Systems**



**A Position Paper Developed by the
Toll Fraud Prevention Committee
of the
Network Operations Forum**

Sponsored by the Alliance for Telecommunications Industry Solutions

**1200 G Street, NW
Suite 500
Washington, DC 20005
(202) 434-8837**

January 1994

The Toll Fraud Prevention Committee of the Alliance for Telecommunications Industry Solutions (formerly the Exchange Carrier Standards Association) has reviewed the problem of remote access fraud at private branch exchanges (PBXs), voice mail systems, and other customer premise equipment (CPE). Such fraud is a serious liability for business customers (and other customers) of telecommunications services, resulting in hundreds of millions of dollars of losses annually. To date, no one can say with any confidence that a solution has been found, or that the problem is under control.

Remote access fraud involves the penetration of a PBX or other CPE by one or more unauthorized callers, typically for the purpose of gaining access to restricted information or to network facilities where the defrauder cannot be charged for resulting calls. PBX remote access fraud is frequently used for "call sell" operations, where people pay defrauders to place unlimited calls to international destinations. Compromised access codes (800 or local numbers which reach Direct Inward System Access [DISA] ports and maintenance ports in the PBXs) have a commercial value of thousands of dollars in the toll fraud underworld. Criminals have a significant incentive, consequently, to penetrate telecommunications equipment for remote access fraud.

In analyzing this problem the TFPC determined that there are many actual or potential participants involved in providing CPE of every type to telecommunications users. It is reasonable to expect that each party will act responsibly when providing such equipment, to ensure that appropriate security against remote access fraud is included. The TFPC identified the following as industry segments that are involved in this issue:

- the business owner
- the consultant
- sales & installation firms
- original equipment manufacturers
- manufacturers of adjunct equipment
- marketers of secondary/refurbished equipment
- local telephone companies
- long distance carriers
- law enforcement agencies
- legislators
- insurers
- consumer/user groups.

Many of these segments may be involved in an individual CPE configuration. The typical PBX goes through many steps: a needs assessment, equipment evaluation, purchase decision, equipment design, installation and testing, maintenance, ongoing use, and eventual retirement/replacement. Thus, it falls to many parties to evaluate the security of a telecommunications environment at progressive steps in the equipment's life cycle.

With this distribution of responsibility, security is often neglected. This simplifies enormously the task of defrauders, who persistently look for CPE with lax security to use for their illegal purposes. It is necessary to stress that the business owner, the owner or lessee of the CPE, has the primary and paramount care, custody, and control of the CPE.

The owner has the responsibility to protect this asset, the telecommunications system, equally as well as other financial assets of the business. The PBX is vital to the business's health, since virtually every business survives and thrives by communicating with other businesses and customers. Abuse of the PBX by hackers, even to the disruption of its functioning, can carry a significant financial and operational penalty. Consequently, the business owner must assure that the PBX (and the entire telecommunications environment under the owner's control) is secure from penetration and abuse.

It is worth noting that this form of telecommunications fraud is a crime. Businesses, whether small firms or large corporations, are persons before the law. They also enjoy the same protections as other citizens, including protection from unlawful disruption of their operations and from theft. Therefore, defrauders of these corporate citizens should be prosecuted to the full extent of the law.

It is essential, therefore, that every industry segment support the integration of security into PBXs, voice mail systems, and other CPE. Some segments have a direct role, as is the case for the equipment manufacturer and the installation firm. Others, such as legislators and regulators, have a less direct, but still important role in the control of toll fraud in general, and remote access fraud in particular. The attachment to this position paper outlines the recommendations of the TFPC for each segment of the industry. For each there is a minimal requirement for preventive action, supported by additional steps that each party should take. These recommendations are not exhaustive of all preventive steps, nor will those that are adopted end remote access fraud. However, they will reduce the risks that industry currently faces.

In the judgment of the TFPC, coordination and cooperation are essential to achieving greater success in this area. Consequently, the TFPC urges each industry segment to deliver the maximum protection that it can identify, in supporting customers of telecommunications services.

ATTACHMENT: SUGGESTED ANTI-FRAUD EFFORTS BY INDUSTRY SEGMENT

RESPONSIBILITIES OF THE BUSINESS OWNER:

The basic responsibility of the business owner is to devote adequate resources (time, talent, capital, etc.) to the selection of CPE and to its management, including fraud prevention, detection, and deterrence. It is an essential part of managing the business. The owner must demand that internal staff and supporting external professionals, such as consultants, include security concerns in the evaluation, design and operation of the telecommunication environment for his/her business.

Other efforts are highly recommended to assure that security matches the importance placed on efficiency, economy, accountability, etc., as considerations in PBX and CPE design.

- Enlist knowledgeable professional support (consultants, security experts) as needed.
- Include security as a prime consideration in the definition of system and user needs.
- Require suppliers to provide only the capabilities required/requested. Other features should be made known, with controls, restrictions, vulnerabilities clearly noted.
- Include security support in maintenance agreements. Identify emergency telephone numbers to be used on discovery or suspicion of fraudulent abuse.
- Define and implement an anti-fraud plan. Enlist employees in the plan; provide a feedback system for emergency alerts. Monitor and refine the plan.
- Manage the telecommunications system when installed: monitor usage continually; assign and encrypt passwords; restrict access in, out, and between interconnected nodes of the system; assure the compatibility and security of interconnected CPE.
- Enlist law enforcement agencies when victimized; preserve evidence for prosecution.
- Secure relevant documentation, to avoid compromise and piracy of data, passwords, etc.
- Secure access to the physical facilities, cabling, access ports, administrative terminals, etc.

RESPONSIBILITIES OF THE CONSULTANT:

The consultant supports the business owner in deciding what type of equipment to buy, what type of services to install, and how to configure both equipment and services for

the desired operational environment. It is the consultant's responsibility frequently to act in place of the owner. Consequently, the consultant has the same tasks as the owner. Trusted for special expertise, the consultant must place high among his/her priorities the establishment of a secure telecommunications environment. This requires that the consultant be very aware of any fraud implications regarding the system being recommended, and ensure that others involved (vendors, installation technicians, etc.) meet or exceed the levels of security needed. The consultant should take steps to ensure that security is cared at the time of installation and into the future.

Additional support efforts are appropriate:

- Understand all current fraud exposures with CPE, and know how to minimize, if not prevent, exposure in the current telecommunications environment.
- Consider security features when making a recommendation on equipment, and detail in writing to the owner the fraud exposure of the final configuration.
- Understand how features in the local and long distance carriers' services can be used to enhance the security of the equipment.
- Be knowledgeable of and make the owner aware of adjunct equipment that can help prevent and identify abuse.

RESPONSIBILITIES OF THE SALES AND INSTALLATION FIRMS:

The sales and installation firms, which will frequently provide ongoing service and maintenance of the CPE, should assist in educating the business owner about the risks and vulnerabilities of the equipment. While stressing the value of the system's features, the sales agents should make known the dangers of toll fraud.

Additional support efforts are appropriate:

- Be completely familiar with the system's features, including those subject to compromise and abuse, such as DISA, maintenance ports, least cost routing features, etc.
- Identify and change any default codes that control access to features and facilities that are subject to compromise and abuse. Secure such replacement codes with responsible management personnel.
- Deactivate features that are not needed, with the full knowledge of the customer.
- Establish time of day restrictions, such as no access to international calling at night and on weekends.
- Restrict access to facilities (WATS, public network "dial 9") and establish calling privileges/limits (internal, local, domestic, international) as appropriate.

RESPONSIBILITIES OF THE MANUFACTURERS OF ORIGINAL AND ADJUNCT EQUIPMENT AND THE MARKETERS OF SECONDARY/REFURBISHED EQUIPMENT:

These industry segments play a special role in protecting the industry from toll fraud. These manufacturers must develop and deploy flexible and effective security protections to complement the advanced telecommunications features required by businesses. In many cases customers are not aware of the need for such protections and do not request them. They are often unaware of the vulnerabilities of an unprotected system and of the dogged drive of the hacker to find new PBXs to abuse.

Additional support efforts are appropriate:

- List in writing for the customer the features and treatments that are necessary to protect against PBX compromise and abuse.
- Ship only those features that the customer requests; remove default passwords from features such as DISA, so that hackers cannot easily access them.
- Secure in writing that the customer is aware of the system's capabilities and protections.
- Provide emergency contact numbers for customers to use in cases of compromise and abuse.
- Make upgrades to the CPE's controlling software by methods more secure than a dial-up modem with default passwords. For example, update the customer's CPE through call back modems or secure token access devices.
- Care for the security and compatibility of adjunct and refurbished equipment with other interconnected segments of the customer's network.
- Educate the customer thoroughly, including support for user groups, etc.

RESPONSIBILITIES OF THE LOCAL TELEPHONE COMPANIES:

The local telephone companies (LECs) have a supporting role for customers who choose their own PBX and CPE. The LECs may frequently not know what a customer is planning. Nor are the LECs familiar with the wide variety of terminal equipment that is available to business owners. However, they can help to combat fraud by promoting an heightened security concern among all their customers.

Other suggested efforts include:

- Conduct wide customer education through bill inserts, addressing end user groups, holding training seminars, etc.
- Evaluate permitted teaming efforts with long distance companies, equipment manufacturers, etc. to educate customers.
- Evaluate all LEC products and services for security concerns before deployment.

- Where tariffed telecommunications systems are offered, fulfill the above suggested security functions of manufacturer and consultant, as appropriate.
- Alert their customer contact personnel (business office, repair, sales/service) to the signs of toll fraud, so that these staffs can better support business owners who are victimized.
- Deploy network blocking services (such as International Direct Dial Blocking) and call screening information digits to complement customer equipment restriction strategies and long distance company network monitoring.
- Develop network monitoring capabilities to highlight potential fraud patterns (local hacking, 800, international, etc.) as early as possible.
- Expand centralized fraud bureau support to a seven day/24 hour basis.
- Continue the use of security staffs to support long distance company investigations and customer inquiries.
- Cooperate with law enforcement agencies in education, investigation, and prosecution efforts.
- Develop case documentation for federal and local regulators, in support of guidelines allowing timely and responsive security efforts in cases of toll fraud.

RESPONSIBILITIES OF THE LONG DISTANCE COMPANIES:

The long distance companies (IXCs) are frequently the networks that bear the brunt of toll fraud, because fraudulent calls are often directed to international destinations. IXCs assist in protecting their customers with a variety of monitoring capabilities and protection (indemnity) plans. IXCs also can combat fraud by continuing the extensive educational campaigns to all customers.

Other suggested efforts include:

- Perform network monitoring of 800 calling and calls directed to international destinations, to identify suspected fraud patterns.
- Alert their customer contact personnel (business office, operator services, repair, sales/service) to the signs of toll fraud, so that these staffs can better support business owners who are victimized.
- Include in their network sales efforts educational security information that will alert customers to network vulnerabilities and suggest effective protections.
- Continue the use of security staffs to support customer inquiries.
- Cooperate with law enforcement agencies in education, investigation, and prosecution efforts.
- Develop case documentation for federal and local regulators, in support of guidelines allowing timely and responsive security efforts in cases of toll fraud.

RESPONSIBILITIES OF REGULATORS:

Regulators perform a critical task in defining how the market acts and reacts. In the case of toll fraud, regulators should recognize that it costs the telecommunications industry (and ultimately consumers and shareholders) billions of dollars annually. Those best able to combat fraud should be empowered to take timely and effective steps to minimize its incidence and severity. In some cases regulatory guidelines might appear to prevent LECs and/or IXCs from disconnecting defrauders in a timely manner. Companies that operate across many states are frequently subject to conflicting rules that do not reflect the realities of systematic, professional toll fraud. Confusion over rules covering collection and security activities allows defrauders to stay on the network. Regulators should act to clarify such areas.

Additional suggestions are:

- Cooperate across jurisdictions (e.g., through NARUC, the FCC) to standardize regulations that allow timely and effective responses against toll fraud.
- Alert customers through periodic press releases about the vulnerabilities of toll fraud and their responsibilities to take effective precautions.
- Stimulate effective legislation punishing toll fraud, and promote its enforcement.
- Allow LECs to deny service, both before it is established and after installation takes place, ~~when warranted by suspected fraud.~~
- Allow telecommunications service providers to cooperate in combating toll fraud through the exchange of customer information.

RESPONSIBILITIES OF LEGISLATORS:

Legislators help create the telecommunications environment in response to the drive of technology and market forces. It is essential that they foster a legislative environment in which telecommunications service providers can bring their full skills to the prevention, detection, and deterrence of toll fraud, recognizing that toll fraud is a professional endeavor that continually adapts.

Other steps are:

- Create no anti-fraud mandates that pit segments of the industry against each other, or that allow one segment to avoid responsibility for contributing to the solution.
- Create incentives for the industry to work cooperatively against the problem.
- Support and finance the efforts of law enforcement organizations, so that they are empowered to pursue and prosecute perpetrators of toll fraud.
- Amend the penal codes to remove the relative impunity enjoyed by those who engage in toll fraud as a profession.

RESPONSIBILITIES OF INSURERS:

Insurers can expand the attention that toll fraud receives by including coverage for toll fraud liability in their product portfolios. Insurers can contribute greatly to the education of business customers by discussing risks and protections related to toll fraud, together or separately with other risk coverage that virtually all businesses consider. Packaging and pricing toll fraud liability coverage affordably (yet profitably) will prompt businesses to take effective precautions. This, in turn, will reduce the incidence of remote access fraud.

RESPONSIBILITIES OF END USER GROUPS:

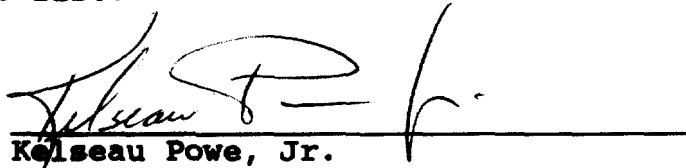
Trade associations and telecommunications end user groups can also broadcast that toll fraud is a significant risk for businesses. Education from many sides will reinforce the necessity for protective action. User groups are particularly valuable in this mode. Frequently, they are aligned by their use of a single technology or a single vendor. Consequently, they can readily share both negative experiences and effective remedies. These groups can also provide the "critical mass" needed to stimulate development of new technology.

RESPONSIBILITIES OF LAW ENFORCEMENT AGENCIES:

While toll fraud might appear as a victimless crime, or one of less pressing priority for prosecution, nevertheless, the operational and financial harm done to businesses by telecommunications defrauders is substantial. Federal and state laws variously define telecommunications fraud and place enforcement responsibilities in many organizations. It is important that this distribution not hinder timely investigations and effective enforcement. Police officers should cooperate across jurisdictions to investigate suspected cases, and district attorneys should prosecute cases to deter future toll fraud and gain restitution for victimized businesses. The enforcement community can also aid the essential educational effort through its own support of end user groups, business councils, etc.

CERTIFICATE OF SERVICE

I, Kelseau Powe, Jr., do hereby certify that on this 14th day of January, 1994, I have caused a copy of the foregoing **COMMENTS OF U S WEST COMMUNICATIONS, INC.**, to be served via first-class United States Mail, postage prepaid, upon the persons listed on the attached service list.


Kelseau Powe, Jr.

***Via Hand-Delivery**

***Reed E. Hundt**
Federal Communications Commission
Room 814
1919 M Street, N.W.
Washington, DC 20554

***Linda Dubroof**
Federal Communications Commission
Room 6008
1919 M Street, N.W.
Washington, DC 20554

***James H. Quello**
Federal Communications Commission
Room 800
1919 M Street, N.W.
Washington, DC 20554

***Informal Complaints and Public
Inquiries Branch**
Federal Communications Commission
Step Code 1600A2
2025 M Street, N.W.
Washington, DC 20554

***Andrew C. Barrett**
Federal Communications Commission
Room 826
1919 M Street, N.W.
Washington, DC 20554

***Gerald P. Vaughan**
Federal Communications Commission
Room 500
1919 M Street, N.W.
Washington, DC 20554

***Ervin S. Duggan**
Federal Communications Commission
Room 832
1919 M Street, N.W.
Washington, DC 20554

***International Transcription
Services, Inc.**
Suite 140
2100 M Street, N.W.
Washington, DC 20037

***Kathleen B. Levitz**
Federal Communications Commission
Room 500
1919 M Street, N.W.
Washington, DC 20554

Albert H. Kramer
Robert F. Aldrich
Douglas E. Rosenfeld
Keck, Mahin & Cate
Penthouse Suite
1201 New York Avenue, N.W.
Washington, DC 20005-3919

APCC

Pamela J. Andrews
Ameritech Operating Companies
Room 4H74
2000 West Ameritech Center Drive
Hoffman Estates, IL 60196

Martin A. Mattes
Richard A. Goldberg
Graham & James
Suite 300
One Maritime Plaza
San Francisco, CA 94111

CPA

Ashley D. Adams
Raymond S. Heyman
O'Connor, Cavanagh, Anderson,
Westover, Killingsworth &
Beshears, P.A.
Suite 1100
One East Camelback Road
Phoenix, AZ 85012-1656

APA

John E. Selent
Hirn Reed & Harper
2000 Meidinger Tower
Louisville, KY 40202

CPMC

Francine J. Berry
American Telephone and Telegraph
Company
Room 3244J1
295 North Maple Avenue
Basking Ridge, NJ 07920

Kenneth A. Hoffman
Laura L. Wilson
Messer, Vickers, Caparello,
Madsen, Lewis, Goldman & Metz,
P.A.
P.O. Box 1876
Tallahassee, FL 32302-1876

FPTAI

John M. Goodman
Edward D. Young, III
Bell Atlantic Telephone Companies
1710 H Street, N.W.
Washington, DC 20006

William E. Wyrrough, Jr.
State of Florida Public Service
Commission
Fletcher Building
101 East Gaines Street
Tallahassee, FL 32399-0850

M. Robert Sutherland
Richard M. Sbaratta
Helen A. Shockey
BellSouth Telecommunications, Inc.
4300 Southern Bell Center
675 West Peachtree Street, N.E.
Atlanta, GA 30375

Gail L. Polivy
GTE Service Corporation
Suite 1200
1850 M Street, N.W.
Washington, DC 20036

Robert McKenna
GTE Service Corporation
HQE03J36
P.O. Box 152092
Irving, TX 75015-2092

Douglas F. Brent
Interexchange Carrier Industry
Committee Toll Fraud Sub-
committee
Suite 700
9300 Shelbyville Road
Louisville, KY 40222

Newton M. Galloway
Mullins & Whalen
P.O. Box 133
Griffin, GA 30224

GPCA

Gregory A. Ludvigsen
Suite 500
706 Second Avenue South
Minneapolis, MN 55402-3006

MIPA

Paul C. Besozzi
Besozzi, Gavin & Craven
Suite 200
1901 L Street, N.W.
Washington, DC 20036

IMRCC

Stephen W. Rimmer
Mississippi Public Communication
Association
1290 Deposit Guaranty Plaza
Jackson, MS 39201

Keith J. Roland
Roland, Fogel, Koblenz & Carr
One Columbia Place
Albany, NY 12223

IPAONYI

Donald J. Elardo
Mary J. Sisak
NCI Telecommunications Corporation
1801 Pennsylvania Avenue, N.W.
Washington, DC 20006

Judith St. Ledger-Roty
Lynn E. Shiporo
Reed Smith Shaw & McClay
1200 18th Street, N.W.
Washington, DC 20036

II

William M. Barvick
Suite 202
240 East High Street
Jefferson City, MO 65101

MICPA

Paul Rodgers
James Bradford Ramsay
NARUC
1102 ICC Building
P.O. Box 684
Washington, DC 20044

St. Louis, MO 63101

Benjamin J. Griffin DOIRMOSC
Lynn E. Shapiro
Reed Smith Shaw & McClay
1200 18th Street, N.W.
Washington, DC 20036

William J. Cowan
New York State Department of
Public Service
Three Empire State Plaza
Albany, NY 12223

Leon M. Kestenbaum
Phyllis A. Whitten
Norina T. Moy
Sprint Communications Company, Inc.
Suite 1100
1850 M Street, N.W.
Washington, DC 20036

Vincent Townsend
North Carolina Payphone Association,
Inc.
Suite 301
3714 Alliance Drive
Greensboro, NC 27404

Martin T. McCue
Linda Kent
United States Telephone Association
Suite 600
1401 H Street, N.W.
Washington, DC 20005-2136

Edward R. Wholl
George J. Brennan
NYNEX Telephone Companies
120 Bloomingdale Road
White Plains, NY 10605

Scott W. Lee UPA
Randle, Deamer, Zarr & Lee, P.C.
Suite 330
139 East South Temple
Salt Lake City, UT 84111

James E. Taylor
Richard C. Hartgrove
John Paul Walters, Jr.
Southwestern Bell Corporation
Room 3520
One Bell Center